



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,499	02/28/2002	Zhichen Xu	100200290-1	7480

7590 10/05/2007
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

WILLIAMS, JEFFERY L

ART UNIT	PAPER NUMBER
----------	--------------

2137

MAIL DATE	DELIVERY MODE
-----------	---------------

10/05/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

MN

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

MAILED

OCT 05 2007

Technology Center 2100

Application Number: 10/084,499
Filing Date: February 28, 2002
Appellant(s): XU ET AL.

Ashok K. Mannava
Reg. No. 45,301
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 6/13/2007 appealing from the Office action
mailed 8/02/06.

1
2 **(1) Real Party in Interest**

3 A statement identifying by name the real party in interest is contained in the brief.

4 **(2) Related Appeals and Interferences**

5 The examiner is not aware of any related appeals, interferences, or judicial
6 proceedings which will directly affect or be directly affected by or have a bearing on the
7 Board's decision in the pending appeal.

8 **(3) Status of Claims**

9 The statement of the status of claims contained in the brief is correct.

10 **(4) Status of Amendments After Final**

11 The appellant's statement of the status of amendments after final rejection
12 contained in the brief is correct.

13 **(5) Summary of Claimed Subject Matter**

14 The summary of claimed subject matter contained in the brief is correct.

15 **(6) Grounds of Rejection to be Reviewed on Appeal**

16 Appellant's brief presents arguments relating to the objection to the specification
17 for failing to provide proper antecedent basis for the claimed subject matter. This issue
18 relates to petitionable subject matter under 37 CFR 1.181 and not to appealable subject
19 matter. See MPEP § 1002 and § 1201.

20 **(7) Claims Appendix**

21 The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Goldschlag et al., "Hiding Routing Information", May 1996, Workshop on
Information Hiding.

Clarke et al., "Freenet: A Distributed Anonymous Information Storage and
Retrieval System", 2000, Lecture Notes in Computer Science.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 42 – 44 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claim 42, appellant recites the limitation "*if a label stored at an intermediate peer of the plurality of peers does not match the predetermined label in the set-up message, the intermediate peer stores the predetermined label and the*

1 *corresponding identity of the next peer*" [emphasis added]. The specification does not
2 provide antecedent basis for storing the predetermined label upon condition that **a label**
3 does not match. The examiner respectfully notes that the claim's recitation, essentially
4 that a peer stores a received label when **a label** stored on a peer does not match the
5 received label, is not in harmony with the appellant's disclosure.

6 Instead, when referencing the specification, it can be clearly seen that a peer
7 compares a received label to stored labels within a hash table. Namely, the hash table
8 is searched so as to determine *if the received label is found as an existing entry* within
9 the hash table (Appellant's disclosure, fig. 7A). However, as now recited, the appellant
10 essentially claims that, regardless of whether or not the received label is found to exist
11 as an entry within the hash table, the peer will store the received label upon the
12 condition that **a label** stored within the hash table does not match the received label. In
13 other words, as long as the hash table contains entries wherein one of the entries ("a
14 label") does not match the received label, then the received will be stored.

15 The examiner respectfully asserts that this is not true operation of the appellant's
16 invention as originally disclosed.

17
18 Claims 43 and 44 are rejected by virtue of dependency.
19
20

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 8 – 12, 20 – 25, 27 – 30, and 42 – 44 are rejected under 35

U.S.C. 102(b) as being anticipated by Goldschlag et al. (Goldschlag), "Hiding Routing Information".

Regarding claim 1, Goldschlag discloses:

forming a path from a provider to a requestor by selecting a plurality of peers in response to receiving a request for information (Goldschlag; page 8, par. 1; page 3, par. 2, lines 4-6; fig. 3 – Herein the method of Goldschlag discloses that a "provider" forms a reply message comprising an "onion" – thus forming a path from the "provider" to a "requester");

updating a table on each peer of said plurality of peers with a respective path index entry for said information (Goldschlag, page 10, par. 4, lines 13-19 – Herein the method of Goldschlag discloses that when each node receives a message, the message [containing a "path index entry" – the listing of the peer index node and all next peer index nodes along the path – each index node identifier encrypted with the

1 public key of the previously identified index node - Goldschlag, page 4, par. 3 – page 5,
2 par. 1; figs. 2, 4] may be stored in a table);

3 *transmitting a message to said requestor through said plurality of peers, said*
4 *message comprising said information and a path index for said information from said*
5 *provider* (Goldschlag, page 3, par. 2, lines 4-6; page 8, par. 1);

6 *and determining a next peer according to said path for said information by*
7 *searching said table of each peer of said plurality of peers with said path index as an*
8 *index into said table* (Goldschlag, page 11, par. 1, lines 8 – 13);

9 *retrieving an identity of said next peer according to said path for said information*
10 *and a respective index peer of said next peer* (Goldschlag, page 11, par. 1, lines 8 – 13
11 – herein the method of Goldschlag comprises each peer searching the table and
12 retrieving identity of the next peer according to the “respective index peer” information
13 that has been indexed in the table);

14 *encrypting said path index with a public key of said respective index peer of said*
15 *next peer to form a next state of said path index; and transmitting a new message with*
16 *said information and said next state of said path index as said path index to said next*
17 *peer* (Goldschlag, page 4, par. 4 – page 5, par. 1 – Herein, Goldschlag discloses that
18 each peer transmits a new message to the next peer. The new message is re-
19 encrypted with the public key of the “respective index peer” found indexed in the table).

20
21 Regarding claim 8, Goldschlag discloses:

1 *forming a respective path message to each peer of said plurality of peers, said*
2 *respective path message comprising said respective path index entry (Goldschlag, page*
3 *10, par. 4).*

4
5 Regarding claim 9, Goldschlag discloses:

6 *The method according to claim 8, wherein said respective path index entry*
7 *comprises an identity of a next peer according to said path, a respective index peer for*
8 *said next peer, and an index entry (Goldschlag, page 6, par. 1; page 10, par. 4).*

9
10 Regarding claim 10, Goldschlag discloses:

11 *wherein said identity of next peer according to said path and said respective*
12 *index peer for said next peer are encrypted with a public key of a peer receiving said*
13 *respective path message (Goldschlag, page 6, par. 1; page 10, par. 4).*

14
15 Regarding claim 11, Goldschlag discloses:

16 *wherein said index entry is formed according to [public.sub.b.sub..sub.j1(. . .*
17 *public.sub.b.sub..sub.j1(public.sub.b.sub..sub.j0(n)) . . .)], where b.sub.j represents said*
18 *respective index peer (Goldschlag, fig. 2; page 5, line 2; fig. 4).*

19
20 Regarding claim 12, it is a method essentially similar to claim 1, and it is rejected,
21 for the same reasons as claim 1, and furthermore because Goldschlag discloses:

1 *updating a respective table of each peer of a plurality of peers with a respective*
2 *path index entry in response to receiving a path formation message containing said*
3 *respective path index entry (Goldschlag; page 2, par. 2 – page 3; page 4, par. 3; page*
4 *10, par. 4, lines 14-18);*

5 *receiving a message comprising said information and a path index; and*
6 *forwarding said information to a next peer in response to a determination of said next*
7 *peer from said table with said path index as a search index into said table (Goldschlag,*
8 *page 11, par. 2).*

9
10 Regarding claim 20, Goldschlag discloses:

11 *receiving said message at said requestor; applying a complementary key to said*
12 *public key of said requestor to said encryption key encrypted with said public key of said*
13 *requestor to obtain said encryption key; applying said encryption key to said encrypted*
14 *reference to retrieve said information (Goldschlag, page 6, par. 2; page 11, par. 2).*

15
16 Regarding claim 21, it is a method essentially similar to the method of claim 1,
17 and it is rejected for the same reasons, and furthermore because Goldschlag discloses:

18 *selecting a path for information from a provider to a requestor through a plurality*
19 *of peers in response to a received request for said information (Goldschlag; page 8,*
20 *par. 1; page 3, par. 2, lines 4-6; fig. 3); receiving a respective set-up message at each*
21 *peer of said plurality of peers, wherein said respective set-up message comprises a*
22 *predetermined label and an identity of a next peer for said information according to said*

1 *path* (Goldschlag, page 10, par. 4, lines 13-19; page 3, par. 2, lines 4-6; page 8, par. 1;
2 – Herein the method of Goldschlag discloses that when each node receives a message,
3 the message [containing a “path index entry” – the listing of the peer index node and all
4 next peer index nodes along the path)

5 *generating an encryption key; encrypting said encryption key with a public key of*
6 *said requestor; encrypting said encryption key with a public key of said provider*

7 (Goldschlag, page 5, line 2; fig. 2; page 3, par. 2, lines 4-6; page 8, par. 2; fig. 4 –

8 Herein, Goldschlag discloses the creation of at least one encryption key, the encryption
9 key transmitted to a responder, wherein the encryption key is encrypted with the
10 responder’s public key so that the responder will have to decrypt the encryption key by
11 using its private key. The responder performs the same in sending a reply message to
12 the requester, wherein the encryption key used to encrypt the reply is encrypted with the
13 requester’s public key);

14 *and encrypting a transaction identifier, a reference for said information, and a first*
15 *next peer according to said path with said encryption key* (Goldschlag, page 5, line 2;
16 page 6, par. 1; page 8, par. 1; page 11, pars. 1, 2). Herein, Goldschlag discloses
17 encrypting with an encryption key *a reference for said information* (such as, payload –
18 pg. 5, line 2), *a transaction identifier* (such as, exp_time_y – a transaction identifier
19 identifying a transferred onion Y and identifying a validity period for said transferred
20 onion Y), and *a first next peer according to said path* (i.e. “Z” – a next peer).

21
22 Regarding claim 22, it is rejected, at least, for the same reasons as claim 1.

1
2 Regarding claim 23, Goldschlag discloses:
3 *receiving a message, wherein said message comprises: an encryption key*
4 *encrypted with a public key of said requestor; said information encrypted with said*
5 *encryption key; and a message label; and retrieving said identity of next peer from said*
6 *table in response to said message label matching said predetermined label in said table*
7 (Goldschlag, page 8, par. 1; page 11, par. 2).

8
9 Regarding claim 24, it is rejected, at least, for the same reasons as claim 2.

10
11 Regarding claim 25, Goldschlag discloses:
12 *comparing said identity of said next peer with a current peer; decrypting said*
13 *encryption key encrypted with a public key of said requestor in response to said identity*
14 *of said next peer being said current peer; and decrypting said information encrypted*
15 *with said encryption key* (Goldschlag, page 11, pars. 1,2).

16
17 Regarding claim 27, Goldschlag discloses:
18 *forming a retrieval message comprising: said encryption key encrypted with said*
19 *public key of said requestor; said encryption key encrypted with said public key of said*
20 *provider; said transaction identifier, said reference for said information, and said first*
21 *next peer according to said path encrypted with said encryption key; and transmitting*

1 *said retrieval message to said provider* (Goldschlag, pages 4, 5; page 6, pars. 1,2; page
2 8, par. 1; page 11, pars. 1, 2).

3
4 Regarding claim 28, Goldschlag discloses:

5 *applying a complementary key of said provider to said encryption key encrypted*
6 *with said public key of said provider; and decrypting said reference for said information,*
7 *said transaction identifier, and said first next peer* (Goldschlag, page 6, pars. 1, 2).

8
9 Regarding claim 29, Goldschlag discloses:

10 *retrieving said information based on said reference for said information;*
11 *encrypting said information with said encryption key; and forming a message label*
12 *based on said transaction identifier* (Goldschlag; page 2, par. 2 – page 3; page 4, par. 3;
13 page 8, par. 1; page 10, par. 4; page 11, pars. 1,2).

14
15 Regarding claim 30, Goldschlag discloses:

16 *forming a message including said encrypted information and said message label;*
17 *and transmitting said message to said first next peer* (Goldschlag, page 11, pars. 1,2).

18
19 Regarding claim 42, it is rejected, at least, for the same reasons as claims 1, 12,
20 and 21, and furthermore because Goldschlag discloses:

21 *if a label stored at an intermediate peer of the plurality of peers does not match*
22 *the predetermined label in the set-up message, the intermediate peer stores the*

1 *predetermined label and the corresponding identity of the next peer* (Goldschlag, page
2 5, par 1). Herein Goldschlag discloses that the intermediate peer stores received
3 messages. A message comprises the label and identity of the next peer. Such is the
4 operation disclosed by Goldschlag and is what will occur *if a label stored at an*
5 *intermediate peer of the plurality of peers does not match the predetermined label in the*
6 *set-up message.*

7 *if a label stored at the intermediate peer matches the predetermined label, the*
8 *intermediate peer retrieves a previously stored message and generates a next state of*
9 *the predetermined label for the setup message* (Goldschlag, page 5, par 1; page 6, par.
10 1, lines 8-18). Herein, Goldschlag discloses that the peer stores "a message" which is
11 retrieved and later utilized for the sending of messages. Goldschlag further discloses
12 that the peer also formats a message utilizing the appropriate data necessary for
13 transmission to the next peer ["generates a next state of the predetermined label"].
14 Such is the operation disclosed by Goldschlag and is what will occur *if a label stored at*
15 *the intermediate peer matches the predetermined label.*

16
17 Regarding claim 43, Goldschlag discloses:

18 *encrypting the received predetermined label with a public key of a respective*
19 *index peer of the next peer* (Goldschlag, page 5).

20
21 Regarding claim 44, Goldschlag discloses:

an encryption key encrypted with the public key of the requester (Goldschlag, fig. 2; page 5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 3 – 7 and 14 – 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldschlag in view of Clarke et al. (Clarke), "Freenet: A Distributed Anonymous Information Storage and Retrieval System".

Regarding claim 3, Goldschlag discloses a system for requesting and retrieving information on a network. The system employs a method for hiding the path (creating an anonymous connection) for such requests and replies (Goldschlag, pages 1-3). Goldschlag discloses the receiving of a request for information, and the formation of a path to said requested information (see rejection of claim 1). Goldschlag, however, does not disclose that the reception for a request for information was at a directory, a determination of availability, or a notification of non-availability.

Clarke similarly discloses a system for requesting and retrieving information, anonymously, on a network. More specifically, Clarke discloses methods for requesting and receiving information, where the information consists of file transactions (Clarke, page 2, par. 1). Because onion routing systems, such as disclosed by Goldschlag, do not focus on the publication, access, and storage of files, Clarke discloses that this system is "best viewed as a complement" to such a onion routing system. Clarke discloses that an additional advantage of such a combination is increased security (Clarke, page 17, table 1, pars. 1-4).

It would have been obvious to one of ordinary skill in the art to employ the methods of Clarke within the system of Goldschlag. This would have been obvious because one of ordinary skill in the art would have known the explicit teachings for the combination of these systems, as well as recognized the benefits of additional security.

Thus, the combination of Goldschlag and Clarke disclose:

receiving said request for information at a directory (Clarke, page 3, par. 3, lines 1-6; page 18, lines 2-6; page 18, par. 2; page 4, pars. 1, 2). Clark discloses that each node acts as a directory containing the locations to requested files.

determining an availability of said information (Clarke, page 6, par. 4);

and notifying said requestor of a determination of non-availability (Clarke, page 6, par. 4). The combination of Goldschlag and Clarke discloses that the method includes notifying the requestor of a decision ("determination") of the quality or state of being non-available ("non-availability") of the requested file. In this case, if the file is available, the method notifies the requester that the file is available - a decision of non-affirmation

1 regarding the quality of the file being non-available. Furthermore, the combination of
2 Goldschlag and Clarke discloses that the method includes notifying a requester that it
3 has been determined that a file is not available on a particular node (Clarke, page 6,
4 par. 5, lines 3,4).

5
6 Regarding claim 4, the combination of Goldschlag and Clarke disclose:
7 *receiving said request for information at a directory* (Clarke, page 3, par. 3, lines
8 1-6; page 18, lines 2-6; page 18, par. 2; page 4, pars. 1, 2). The combination of
9 Goldschlag and Clarke discloses that each node acts as a directory containing the
10 locations to requested files.

11 *determining an availability of said information* (Clarke, page 6, par. 4);
12 *and generating an encryption key in response to a determination of said*
13 *availability* (Clarke, page 3, par. 3, lines 1-6; page 18, lines 2-6; page 18, par. 2; page 4,
14 pars. 1, 2). The combination of Goldschlag and Clarke discloses that when a file is
15 found to be available on a remote node, the request for the file is forwarded to the
16 remote node. When such requests are forwarded, the combination of Goldschlag and
17 Clarke discloses that these requests are link encrypted with an encryption key. The
18 process of encrypting a request with an encryption key clearly results in the process of
19 coming into being (the "generation") of an encryption key, whether the key is produced
20 from storage, received over a network, or the resultant of a key-derivation algorithm
21 (Goldschlag, fig. 1; page 10, par. 3).

1 Regarding claim 5, the combination of Goldschlag and Clarke disclose:
2 *determining a first next peer from said provider and a respective index peer for*
3 *said first next peer according to said path; and encrypting a reference to said*
4 *information, said first next peer, and said respective index peer of said first next peer*
5 *with said encryption key* (Goldschlag, page 6, par. 1).

6
7 Regarding claim 6, the combination of Goldschlag and Clarke disclose:
8 *wherein said encryption key is generated according to a DES encryption*
9 *algorithm.* Goldschlag discloses using a efficient symmetric algorithm for the encryption
10 key, however, Goldschlag does not specify DES encryption. It would have been
11 obvious to use DES encryption as this is an efficient algorithm used in the onion routing
12 system as evidenced by Goldschlag, "Anonymous Connections and Onion Routing",
13 page 6, section E – Onions).

14
15 Regarding claim 7, the combination of Goldschlag and Clarke disclose:
16 *encrypting said encryption key with a public key of said requestor; encrypting*
17 *said encryption key with a public key of said provider; forming a provider message,*
18 *wherein said provider message comprises: said encryption key encrypted with said*
19 *public key of said requestor; said encryption key encrypted with said public key of said*
20 *provider; said encrypted reference; and said encrypted first next peer and said*
21 *respective first index peer; and transmitting said message to said provider* (Goldschlag,
22 page 6, section 3.1).

Regarding claim 14, it is rejected, at least, for the same reasons as claim 3.

Regarding claim 15, it is rejected, at least, for the same reasons as claims 4 and 5.

Regarding claim 16, it is rejected, at least, for the same reasons as claims 4 – 7.

Regarding claim 17, it is rejected, at least, for the same reasons as claim 6.

Regarding claim 18, the combination of Goldschlag and Clarke disclose:
receiving said second message at said provider; applying a complementary key to said public key of said provider to said obtain said encryption key; and applying said encryption key to said encrypted reference to retrieve said reference (Goldschlag, page 6, section 3.1).

Regarding claim 19, it is rejected, at least, for the same reasons as claim 7, and furthermore because the combination of Goldschlag and Clarke disclose the retrieving of information based upon a reference (a request for said information) (Clarke, section 3.2).

1 **(10) Response to Argument**

2 Appellant argues primarily that:

3
4 (i) *Regarding the objection with respect to claim 42, the specification clearly*
5 *discloses that the peer privacy module 220 at an intermediate peer may be configured*
6 *to search the hash table 225 for an existing entry matching the received current label. If*
7 *the existing entry is not present, the hash table 225 may be updated...* (Arguments, pg.
8 17)

9 *The rejection of claim 42-44 under 112 first paragraph for lack of written*
10 *description was based upon the objection to the specification...As described above, the*
11 *specification clearly discloses the features of claims 42 and 44...* (Arguments, pg. 18,
12 par. 3)

13
14 In response, examiner respectfully points out that the appellant essentially recites
15 within claim 42 that the peer will store the received label upon the condition that **a label**
16 stored within the hash table does not match the received label. This recited operation is
17 not equivalent to the appellant's argument "If **the existing entry** is not present, the
18 hash table 225 may be updated...". Namely, as recited, the appellant claims that,
19 regardless of whether or not the received label is found to exist as an entry within the
20 hash table, the peer will store the received label upon the condition that any label stored
21 within the hash table does not match the received label. In other words, as long as the

1 hash table contains entries, wherein one of the entries ("a label") does not match the
2 received label, then the received will be stored.

3 In response to applicant's argument that the references fail to show certain
4 features of applicant's invention, it is noted that the features upon which applicant relies
5 (i.e., If ***the existing entry*** is not present, the hash table 225 may be updated...) are not
6 recited in the rejected claim(s). Although the claims are interpreted in light of the
7 specification, limitations from the specification are not read into the claims. See *In re*
8 *Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

9 As the appellant's argument is not in harmony with the claim language and the
10 appellant has not pointed out support for the language as claimed, the examiner does
11 not find the appellant's argument to be persuasive.

12
13 (ii) *Regarding ... claim 44 the specification clearly discloses an encryption key*
14 *encrypted with the public key of the requestor.* (Arguments, pg. 18, par. 2)

15
16 In response, the examiner respectfully notes that the appellant appears to have
17 shown evidence within the appeal brief for support of the claim recitation "an encryption
18 key encrypted with the public key of the requester". As such, the examiner withdraws
19 the rejection of claim 44 under 112, first paragraph.

20

1 (iii) *There are no index peers in Goldschlag, and accordingly, Goldschlag fails to*
2 *teach a respective index peer and encrypting the path index with public key of the index*
3 *peer of the next peer.* (Arguments, pg. 20, par. 3)

4
5 In response, the examiner respectfully asserts that Goldschlag does teach "index
6 peers". The method of Goldschlag necessitates the construction of an onion indicating
7 every index peer along the path from one end of a network to the other (Goldschlag,
8 figs. 3, 2, 4). These onions, and thus the index peers are indexed in a table stored on
9 each of the peer nodes within the network path (Goldschlag, pg. 5, par. 1; pg. 10, par.
10 3). Therefore, Goldschlag clearly teaches "index peers".

11
12 (iv) *An index peer for a next node is not disclosed in Goldschlag and using a public*
13 *key of an index peer for a next node is not disclosed in Goldschlag.* (Arguments, pg.
14 21, par. 3)

15
16 In response, the examiner respectfully notes that Goldschlag does teach "index
17 peers" as indicated directly above regarding argument (iii). Furthermore, the examiner
18 points out that the method of Goldschlag comprises each peer searching a table and
19 retrieving identity of the next peer according to the "respective index peer" information
20 that has been indexed in the table, and re-encrypting the "onion" with the proper public
21 key corresponding to the "respective peer information" (Goldschlag, page 11, par. 1,
22 lines 8 – 13; page 5, lines 1-4)

1
2 (v) *Also, claim 11 is directed to an index entry including respective index peers,*
3 *which is not taught by Goldschlag.* (Arguments, pg. 22, par. 1)
4

5 In response, the examiner respectfully points out that the method of Goldschlag
6 necessitates the construction of an onion indicating every index peer along the path
7 from one end of a network to the other (Goldschlag, figs. 3, 2, 4). These onions, and
8 thus the index peers are indexed in a table stored on each of the peer nodes within the
9 network path – thus creating “index entry” (Goldschlag, pg. 5, par. 1; pg. 10, par. 3).
10

11 (vi) *Firstly, Goldschlag fails to disclose a public key associated with the identity*
12 *information for a next node. ... Secondly ... Goldschlag fails to teach identity information*
13 *that is an index peer for a next node.* (Arguments, pg. 23, lines 4 – 8)
14

15 In response, the examiner respectfully notes that Goldschlag discloses that each
16 node encrypts the message with the public key associated with the next node, the next
17 node being identified by its index peer information that has been indexed in a table
18 (Goldschlag, pg. 5, lines 1,2, par. 1; pg. 10, par. 2).
19

20 (vii) Goldschlag fails to teach index peers for the routing nodes, and encrypting
21 messages with a public key of a respective index peer for a routing node. (Arguments,
22 pg. 23, lines 10-11).

1
2 In response, the examiner respectfully notes, as previously indicated in response
3 to the arguments above, that Goldschlag clearly teaches that nodes have "index peers"
4 and that the messages transmitted to those "index peers" are encrypted with the public
5 key of the appropriate "index peer".

6
7 (viii) *Hence, Goldschlag fails to teach encrypting said encryption key with a public key*
8 *of said provider.* (Arguments, pg. 25, par. 1)

9
10 In response, the examiner respectfully notes that Goldschlag discloses the
11 creation of at least one encryption key, the encryption key transmitted to a responder
12 ("provider"), wherein the encryption key is encrypted with the responder's public key so
13 that the responder will have to decrypt the encryption key by using its private key
14 (Goldschlag, page 5, line 2; fig. 2; page 3, par. 2, lines 4-6; page 8, par. 2; fig. 4). Thus,
15 Goldschlag discloses encrypting the encryption key with a public key of the provider.

16
17 (ix) *However, the expiration time is not an identifier of a transaction ... Because*
18 *Goldschlag fails to teach using the expiration time as an identifier, Goldschlag fails to*
19 *teach encrypting a transaction identifier.* (Remarks, pg. 25, par. 2)

20
21 In response, the examiner points out that Goldschlag discloses that the
22 expiration time is a value assigned to the message, and it is used by each node to

1 identify a valid transaction (Goldschlag, pg. 5, par. 1; pg.10, par. 4). Thus, the assigned
2 value is a transaction identifier or "*an identifier of a transaction*". The examiner, further
3 notes that the applicant also discloses the that the transaction identifier is an assigned
4 value, the value similarly being a counter value associated with the transaction and
5 used as a basis for transmitting messages (Appellant's specification, pg. 20, lines 5-10,
6 15, 16; pg. 21, lines 5-7).

7
8 (x) *However, Goldschlag fails to teach the payload comprises a reference to*
9 *requested information.* (Arguments, pg. 25, par. 3)

10
11 In response, the examiner respectfully points out that the entire purpose of the
12 communicated messages is for the receiving of requested information. Thus the
13 encrypted messages are references for requested information (Goldschlag, pg. 2, par. 2
14 – pg. 3, par. 2).

15
16 (xi) *There is no comparison performed in Goldschlag to determine whether there is a*
17 *match... Accordingly, these features are not taught by Goldschlag...* (Arguments, pg.
18 26, par. 2).

19
20 In response to applicant's argument that the references fail to show certain
21 features of applicant's invention, it is noted that the features upon which applicant relies
22 (i.e., a "comparison performed" or performing a comparison to determine...) are not

1 recited in the rejected claim(s). Although the claims are interpreted in light of the
2 specification, limitations from the specification are not read into the claims. See *In re*
3 *Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

4
5 (xii) *Neither Clarke nor Goldschlag discloses a peer similar to the directory 130, and*
6 *furthermore, Clarke fails to disclose that each node in the peer-to-peer network would*
7 *have to know a path between itself and a requestor.* (Arguments, pg. 28, par. 2)

8
9 In response to applicant's argument that the references fail to show certain
10 features of applicant's invention, it is noted that the features upon which applicant relies
11 (i.e., *a peer similar to the directory 130, and each node in the peer-to-peer network*
12 *would have to know a path between itself and a requestor*) are not recited in the
13 rejected claim(s). Although the claims are interpreted in light of the specification,
14 limitations from the specification are not read into the claims. See *In re Van Geuns*, 988
15 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

16
17 (xiii) Thus, there is unreasonable expectation of success when combining the onion
18 routing of Goldschlag with Clarke.

19
20 In response, the examiner respectfully notes that the prior art clearly expects a
21 measure of success in the combination of the methods of Clarke with the onion-routing

disclosed by Goldschlag, as indicated by the explicit teachings that such methods are
complementary (Clarke, pg. 2, par. 3).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the
Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.


Respectfully submitted,

Jeffery Williams



Conferees:

Gilberto Barron


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

/Benjamin Lanier/
Benjamin Lanier
Examiner Art Unit 2132